UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/944,694	08/31/2001	Matthew Gast	NC30561	2124

7590 09/28/2006

Brian T. Rivers, Esq.
Nokia, Inc.
Mail drop 1-4-755
6000 Connection Dr.
Irving, TX 75039

EXAMINER	
HA, LEYNNA A	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 09/28/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/944,694	GAST, MATTHEW	
	Examiner	Art Unit	
	LEYNNA T. HA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 April 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-18 are pending.

2. This is a Non-Final rejection.

4. In view of the Pre-Brief conference request filed on 4/3/2006, PROSECUTION IS HEREBY REOPENED. A non-final rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 3 and 12-18 are rejected under 35 U.S.C. 102(e) as being anticipated by Binding, et al. (US 6,775,772).

As per claim 3:

Binding, et al. discloses a system for providing network security, comprising:

means for receiving a request to perform a cryptographic operation; **(col.16, lines 36-42)**

means for returning a response to the cryptographic operation request; **(col.15, lines 59-61)**

means for translating a first plurality of cleartext data into a second plurality of cleartext data in accordance with at least one translation rule; and **(col.4, lines 54-60 and col.15, lines 37-39; the claimed means for translating can broadly be interpreted as changing from one form of data to another form or to decipher/decrypt encrypted data into its decrypted (original or cleartext) data. Binding teaches message (col.15, line 37) which contains plurality of data is decrypted which is the first plurality of decrypted (cleartext) data. Then Binding explains a second decryption (col.15, lines 38-39) is performed resulting in a**

second plurality of decrypted (cleartext) data. Thus, the second decryption of the decrypted data reads on translating a first plurality of cleartext data into a second plurality of cleartext data.)

at least one module for performing said cryptographic operations, said cryptographic operations including obtaining the first plurality of cleartext data based upon a first plurality of encrypted data **(col. 15, lines 27-29 and 33-34)**, and encrypting the second plurality of cleartext data to obtain a second plurality of encrypted data. **(col.15, lines 47-52)**

As per claim 12: See col.9, lines 64-65; discussing at least one cryptographic module is a cryptographically strong pseudorandom number generator.

As per claim 13: See col.14, lines 54-56 and col.15, lines 43-51; discussing the cryptographic operations are performed using cryptographic acceleration hardware.

As per claim 14: See col.15, lines 1-5; discussing the cryptographic acceleration hardware includes a plurality of individual hardware acceleration units.

As per claim 15: See col.14, lines 54-56 and col.15, lines 43-51; discussing at least one individual hardware acceleration unit is dedicated to one function.

As per claim 16: See col.10, lines 5-10; discussing the cryptographic acceleration hardware is updateable by loading at least one cryptographically signed instruction.

As per claim 17: See col.12, lines 46-53; discussing the cryptographic acceleration hardware is tamper-resistant.

As per claim 18: See col.12, lines 46-53; discussing the cryptographic acceleration hardware is tamper-evident.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1, 2 and 4-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Grabelsky, et al. (US 7,032,242), and further in view of Zarom (US 6,356,529).

As per claim 1:

Grabelsky, et al. discloses a method for providing network security, comprising the steps of:

receiving a plurality of network protocol packets, wherein a network protocol packet includes a network protocol header **(col.20, lines 49-50)** and a plurality of network protocol data, and wherein the network protocol data include a first cryptographic protocol header **(col.21, lines 17-21)** and a first plurality of encrypted data, at least a portion of at least some of the network protocol packets being configured in accordance with a transport layer protocol or a network layer protocol; **(col.11, lines 55-56)**

determining a first plurality of cryptographic protocol rules associated with the network protocol data; **(col.21, lines 4-13 and col.22, lines 63-55)**

establishing a cryptographic session, if required by said first cryptographic rules; **(col.24, lines 34-40)**

applying the first plurality of cryptographic protocol rules to the first encrypted data to obtain a first plurality of cleartext data; **(col.23, lines 49-57)**

[translating the first plurality of cleartext data into a second plurality of cleartext data in accordance with at least one translation rule]

encrypting the second plurality of cleartext data in accordance with at least one rule associated with a second cryptographic protocol, resulting in a second plurality of encrypted data. **(col.23, lines 27-37)**

However, Grabelsky did not provide translating the first plurality of cleartext data into a second plurality of cleartext data in accordance with at least one translation rule.

Zarom discloses a method and system for translating data transmitted according to the WAP network protocols in the lower protocol layers rather than requiring the packet to be transformed into higher layers (col.4, lines 52-64). Zarom discloses there is an increasing demand for different types of communication services through the increasing popular portable electronic devices (col.1, lines 14-22) that there is a need to extend the power and efficacy of operation of portable, wireless electronic communication devices. WAP (wireless application protocol) has been developed and designed to efficiently provide both multimedia and telephony services to wireless communication devices (col.1, lines 24-33) and provides the required adaptations and modifications to such software and data transmission protocols. Such adaptations and modifications includes a translation system or gateway to translate HTML to form WML

(col.1, lines 54-62). Zarom further suggests that current available translators in the art require the data to be translated only at the highest (application) level of the network protocols and involves two separate sessions are operated with significant delays in each session for the translation process (col.6, lines 28-32), where the proxy server waits for the translation process to be completed for each of original server and wireless communication device client before the translated data can be passed to the other session (col.2, lines 20-34 and col.3, lines 15-17). Thus, this method significantly decreases the efficiency of these background art translators and their translation process (col.2, lines 37-39 and col.6, lines 28-32). However, Zarom' solution would be able to pass translated information as soon as only a portion is translated according to rules (col.3, lines 8-15 and col.7, lines 12-30) and the translation process is performed entirely at the IP level rather than at the application level (col.6, lines 21-28). Zarom teaches data must be converted through all of the network layers before translation and must be reconverted to a format which is suitable for transmission through the physical network media (col.2, lines 23-28). Thus, is more efficient which is able to translate packets more rapidly from protocol type to the other than background art translators (col.2, lines 40-54 and col.6, lines 32-34). Zarom discloses the translator receiving either regular IP packets and WAP packets or other wireless network packets (col.7, lines 32-34). Zarom shows the examples of cleartext data into another cleartext data or (language) format translated to another format (col.3, lines 26-37): HTML to WML (col.1, lines 57-58), TCP packets to WTP packets (col.7, lines 58-60), WAP to TCP packets (col.9, lines 40-50), IP packet to a WAP network packet (col.6, lines 55-58).

Therefore, it would have been obvious for a person of ordinary skills in the art at the time of the invention was made to combine the teaching of Grabelsky with the teaching of translating the first plurality of cleartext data into a second plurality of cleartext data in accordance with at least one translation rule as taught by Zarom because translating at IP level is faster and efficient in order to effectively to communicate deliver content from the Internet (col.1, lines 50-63 and col.6, lines 21-35).

As per claim 2:

Grabelsky discloses a system for providing network security, comprising:

an input module for receiving a plurality of network protocol packets **(col.20, lines 49-50)**, at least a portion of at least some of the network protocol packets being configured in accordance with a transport protocol or a network layer protocol; **(col.11, lines 55-56 and col.21, lines 17-21)**

(a translation module for translating a first plurality of data into a second plurality of data)

an output module; and **(col.23, lines 21-22)**

a cryptographic module responsive to the input module and the output module for performing cryptographic operations. **(col.23, lines 49-62)**

However, Grabelsky did not provide a translation module for translating a first plurality of data into a second plurality of data.

Zarom discloses a method and system for translating data transmitted according to the WAP network protocols in the lower protocol layers rather than requiring the packet to be transformed into higher layers (col.4, lines 52-64). Zarom discloses there

is an increasing demand for different types of communication services through the increasing popular portable electronic devices (col.1, lines 14-22) that there is a need to extend the power and efficacy of operation of portable, wireless electronic communication devices. WAP (wireless application protocol) has been developed and designed to efficiently provide both multimedia and telephony services to wireless communication devices (col.1, lines 24-33) and provides the required adaptations and modifications to such software and data transmission protocols. Such adaptations and modifications includes a translation system or gateway to translate HTML to form WML (col.1, lines 54-62). Zarom further suggests that current available translators in the art require the data to be translated only at the highest (application) level of the network protocols and involves two separate sessions are operated with significant delays in each session for the translation process (col.6, lines 28-32), where the proxy server waits for the translation process to be completed for each of original server and wireless communication device client before the translated data can be passed to the other session (col.2, lines 20-34 and col.3, lines 15-17). Thus, this method significantly decreases the efficiency of these background art translators and their translation process (col.2, lines 37-39 and col.6, lines 28-32). However, Zarom' solution would be able to pass translated information as soon as only a portion is translated according to rules (col.3, lines 8-15 and col.7, lines 12-30) and the translation process is performed entirely at the IP level rather than at the application level (col.6, lines 21-28). Zarom teaches data must be converted through all of the network layers before translation and must be reconverted to a format which is suitable for transmission through the physical

network media (col.2, lines 23-28). Thus, is more efficient which is able to translate packets more rapidly from protocol type to the other than background art translators (col.2, lines 40-54 and col.6, lines 32-34). Zarom discloses the translator receiving either regular IP packets and WAP packets or other wireless network packets (col.7, lines 32-34). Zarom shows the examples of cleartext data into another cleartext data or (language) format translated to another format (col.3, lines 26-37): HTML to WML (col.1, lines 57-58), TCP packets to WTP packets (col.7, lines 58-60), WAP to TCP packets (col.9, lines 40-50), IP packet to a WAP network packet (col.6, lines 55-58).

Therefore, it would have been obvious for a person of ordinary skills in the art at the time of the invention was made to combine the teaching of Grabelsky with the teaching of translating the first plurality of cleartext data into a second plurality of cleartext data in accordance with at least one translation rule as taught by Zarom because translating at IP level is faster and efficient in order to effectively to communicate deliver content from the Internet (col.1, lines 50-63 and col.6, lines 21-35).

As per claim 4: **See Zarom on col.3, lines 8-15 and col.7, lines 12-30;** discussing at least one translation rule is predetermined.

As per claim 5: **See Zarom on col.7, lines 12-30 and 55-67;** discussing at least one translation rule is determined dynamically.

As per claim 6: **See Zarom on col.3, lines 5-6;** discussing the first cryptographic protocol is WTLS.

As per claim 7: **See Zarom on col.5, lines 37-46;** discussing the first plurality of encrypted data is associated with WML.

As per claim 8: **See Zarom on col.3, lines 57-58;** discussing second plurality of encrypted data is associated with HTML.

As per claim 9: **See Zarom on col.8, lines 7-11;** discussing the second cryptographic protocol is SSL over HTTP.

As per claim 10: **See Grabelsky on col.22, lines 62-65 and col.23, lines 50-62;** discussing the first cryptographic protocol and the second cryptographic protocol are identical.

As per claim 11: **See Grabelsky on col.22, lines 62-65 and col.23, lines 50-62;** discussing the first plurality of encrypted data and the second plurality of encrypted data conform to different revisions of a specification for the same cryptographic protocol.

Response to Arguments

Claims 3 and 12-18 remains rejected over Binding, et al. Claim 3 recites cryptographic operation request and response wherein the cryptographic operations includes obtaining the first plurality of cleartext data based upon a first plurality of encrypted data and encrypting the second plurality of cleartext data to obtain the second plurality of encrypted data. In addition, claim 3 recites translating a first plurality of cleartext data into a second plurality of cleartext data in accordance with a translation rule. Claim 3 does not have the limitations of claims 1 and 2, which is receiving network protocol packets where at least a portion of at least some of the network protocol packets being configured in accordance with a transport layer protocol or a network

layer protocol and determining and applying the cryptographic rules to the encrypted data. Therefore, claim 3 does not claim any types of packets or the protocol in the matter but is merely cryptographic operations which involves encryption and decryption of plurality of data.

Further, Examiner acknowledges applicants interpretation for means for translating which is to change from one form to another. Applicant's interpretation of translating of first cleartext data into a second cleartext data does not limit to the examples of WML data translated into the HTML data or change from one format/language into another format. Translating can also be given as to decipher/decrypt encrypted data into its decrypted (original or cleartext) data or a combination of the same type of cryptographic operations. Thus, examiner traverses applicant's argument that Binding first decode data is the same as the second decoded data (i.e. parameter → parameter). Binding teaches a message which contains plurality of data is decrypted (col.15, line 37) which is the first plurality of decrypted (cleartext) data. Then Binding explains a second decryption (col.15, lines 38-39) is performed resulting in a second plurality of decrypted (cleartext) data. Thus, the second decryption of the decrypted data reads on translating a first plurality of cleartext data into a second plurality of cleartext data (col.4, lines 54-60 and col.15, lines 37-39).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

LHa

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100